Daniel Schafer
CEO bei BLS AG
und Vorstandsmitglied
bei Electrosuisse

Digitalisierung bei der Bahn

Die Digitalisierung ist aus der Bahnwelt nicht mehr wegzudenken. Stellwerke sind digital zentralisiert, die Zugbeeinflussung erfolgt durch das ETCS und für die Instandhaltung überwachen Sensoren die Komponenten und Züge. Erkannte Störungen lösen automatisiert Behebungsprozesse aus. Die Wartung der Fahrzeuge ist nicht mehr ohne ERP-Systeme möglich, die eine detaillierte Wartungsplanung und ein effizientes Ersatzteilmanagement ermöglichen.

Operational-Technology-Systeme (OT) wurden meist vor Jahren für eine lange Einsatzdauer konzipiert. Sie sind heute oft veraltet, kommunizieren über unsichere Protokolle und weisen schwer behebbare Softwareschwachstellen auf. Häufig fehlen zudem wichtige Authentisierungsfunktionen. Da solche Systeme bis dato meist in isolierten Umgebungen betrieben wurden und der Fokus vor allem auf den funktionalen Aspekten lag, fehlt es heutigen Anbietern und Herstellern am Bewusstsein für Cybergefahren – ganz im Gegensatz zur IT-Welt, die sich damit schon lange auseinandersetzt.

Digitalisierung und Automatisierung vernetzen heute IT und OT zunehmend. Die klaren Grenzen von früher verschwinden zusehends. Industrieanlagen, oder eben die Eisenbahn, sind zunehmend Cybergefahren ausgesetzt, ohne dafür gewappnet zu sein. So kann beispielsweise bereits die Fernwartung mit einem Malware-verseuchten PC zu grossem Schaden führen.

Deshalb ist es entscheidend, dass wir angemessene Sicherheitsmassnahmen implementieren. Dort, wo wir die Resilienz der Systeme nicht direkt verbessern können, müssen wir flankierende Massnahmen ergreifen, wie die Aufteilung der Systeme in Sicherheitszonen und eine konsequente Zugriffskontrolle an den Zonenübergängen. Aber auch die Hersteller und Anbieter sollten wir vermehrt verpflichten, sicherere Anlagen auszuliefern, denn hier wäre deutlich mehr möglich: Fast alle bewährten Konzepte aus der IT-Sicherheit lassen sich nämlich auch in der OT-Welt anwenden, da weniger die Technik, sondern vielmehr die Anwendungsszenarien die Unterschiede zwischen IT und OT bestimmen.

Numérisation dans les chemins de fer

La numérisation est devenue essentielle dans le domaine ferroviaire. Les postes d'aiguillage sont centralisés numériquement, le contrôle des trains est assuré par l'ETCS – le système européen de contrôle des trains – et, pour la maintenance, des capteurs surveillent les composants et les trains. Les défaillances détectées déclenchent automatiquement des processus de dépannage. La maintenance des trains n'est plus possible sans les systèmes ERP, qui permettent une planification détaillée de la maintenance et une gestion efficace des pièces de rechange.

Les systèmes OT (technologie opérationnelle) ont généralement été conçus il y a des années pour une longue durée d'utilisation. Aujourd'hui, ils sont souvent obsolètes, communiquent via des protocoles peu sûrs et présentent des faiblesses logicielles auxquelles il est difficile de remédier. De plus, d'importantes fonctions d'authentification font souvent défaut. Comme ces systèmes étaient jusqu'à présent généralement exploités dans des environnements isolés et que l'accent était surtout mis sur les aspects fonctionnels, les fournisseurs et les fabricants actuels n'ont pas pris suffisamment conscience des cyberdangers – contrairement au monde informatique qui s'y intéresse depuis longtemps.

La numérisation et l'automatisation mettent aujourd'hui de plus en plus l'IT et l'OT en réseau. Les frontières claires d'autrefois disparaissent à vue d'œil. Les installations industrielles, ou même les chemins de fer, sont de plus en plus exposés aux cyberdangers, sans être armés pour y faire face. Par exemple, la maintenance à distance peut déjà, par le biais d'un PC infecté par un logiciel malveillant, entraîner des dommages importants.

Il est donc crucial de mettre en œuvre des mesures de sécurité appropriées. Là où il n'est pas possible d'améliorer directement la résilience des systèmes, des mesures d'accompagnement doivent être prises, comme la répartition des systèmes dans des zones de sécurité et un contrôle d'accès conséquent pour passer d'une zone à l'autre. Mais nous devrions également obliger davantage les fabricants et les fournisseurs à livrer des installations plus sûres, car il serait possible de faire nettement plus à ce niveau : presque tous les concepts éprouvés de la sécurité informatique peuvent en effet être appliqués dans le domaine de l'OT, car ce n'est pas tant la technique que les scénarios d'application qui déterminent les différences entre l'IT et l'OT.